# Contratación de servicios educativos en la nube.

# Riesgos y recomendaciones desde la perspectiva de la protección de datos personales

Mariana Fossatti y Patricia Díaz

(datysoc.org)

Actualmente se observa una enorme irrupción de servicios de tecnología educativa basados en el cloud computing, así como la creciente interoperabilidad de estos servicios. De estas tecnologías surgen muchas posibilidades de innovación en el ámbito educativo, pero también diversas incertidumbres y desafíos. El almacenamiento y la posibilidad de tratamiento masivo de datos de estudiantes permite acumular información y generar perfiles personales desde la temprana edad en que comienzan la actividad escolar y durante todo su tránsito educativo. En este nuevo contexto surge la disyuntiva entre confiar ciegamente en las soluciones tecnológicas o analizarlas con una mirada crítica que permita evaluar sus implicancias legales y éticas.

En el marco de la investigación sobre "Privacidad y protección de datos en la educación pública uruguaya" que nos encontramos desarrollando para Datysoc.org[1] hemos detectado la necesidad por parte de las autoridades e instituciones educativas (IEs) uruguayas de contar con mayor información sobre las tecnologías educativas que contratan. Las IEs deben saber responder, al menos, estas preguntas: ¿qué es la computación en la nube?, ¿qué aspectos evaluar al momento de optar por las diferentes soluciones de tecnología educativa disponibles?, ¿cuáles son los principales riesgos en materia de privacidad y protección de datos personales?

1DATYSOC: Grupo de investigación que busca proporcionar una evaluación del estado actual del arte de la vigilancia de las comunicaciones, de la privacidad y de la ciberseguridad en Uruguay (http://datysoc.org/).

Entendiendo que las soluciones tecnológicas no son neutras, sino que su estructura y gobernanza inciden en el ejercicio de los derechos de los usuarios, describiremos el funcionamiento de los diferentes modelos de servicios educativos en la nube, la responsabilidad que, de acuerdo a la Ley de Protección de Datos Personales de Uruguay, asumen las IEs al momento de contratar estos servicios y los principales riesgos. Finalmente presentaremos algunas recomendaciones.



## 1- ¿Qué es la computación en la nube?

Si bien no existe una definición universalmente aceptada de computación en la nube o "Cloud Computing", existen organismos internacionales cuyos objetivos son la estandarización de Tecnologías de la Información, y específicamente de las tecnologías basadas en la nube. El

Information Technology Laboratory del NIST (Agencia del departamento de comercio de los Estados Unidos) se encarga de los estándares de las tecnologías de la información y define al Cloud Computing como:

> "Un modelo que permite el acceso bajo demanda a través de la Red a un conjunto compartido de recursos de computación configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar rápidamente con el mínimo esfuerzo de gestión o interacción del proveedor del servicio" (Traducción nuestra)

Este modelo implica la posibilidad de que los diferentes recursos físicos (como por ejemplo almacenamiento, procesamiento, memoria, ancho de banda de la red y máquinas virtuales) sean asignados y reasignados dinámicamente, de modo que el cliente, normalmente, no tiene control ni conocimiento sobre la posición exacta de los recursos proporcionados.

## 2 - Modelos de computación en la nube según tipo de acceso

De las diferentes clasificaciones de modelos de computación en la nube[2] realizadas por el Information Technology Laboratory del NIST, nos interesa particularmente describir la clasificación relacionada con el *tipo de acceso*, ya que este condiciona la posibilidad de control efectivo de los datos.

De acuerdo a esta clasificación, encontramos que los centros de datos virtualizados pueden utilizar modelos de nube privada, nube pública o nube híbrida.

La «**nube privada**» es una infraestructura informática (máquinas, redes, almacenamiento, centros

2Además de la clasificación de servicios cloud según el acceso, encontramos la clasificación de **"modelos por tipo de servicio"** que suelen aplicarse a las soluciones en nube, tanto públicas como privadas. Estos son: 1) IaaS («Cloud Infrastructure as a Service», infraestructura como servicio), 2) SaaS («Cloud Software as a Service», programa informático como servicio), 3) PaaS («Cloud Platform as a Service», plataforma como servicio).

de datos, etc) dedicada a una organización individual; está situada en las instalaciones de la propia organización o bien su gestión está subcontratada a un tercero (normalmente a través de alojamiento de servidores). Una de las características que hace atractiva este tipo de nube para una organización, es el grado de control y de privacidad de los datos, ya que los recursos se encuentran bajo el estricto control de la propia organización (no nos referimos al grado de seguridad pues la seguridad depende de varios factores).

Una «**nube pública**», por el contrario, es una infraestructura propiedad de un proveedor especializado en la prestación de servicios de nube que pone a disposición (y, por consiguiente, comparte) sus sistemas con los usuarios u organizaciones que contratan sus servicios. Se accede al servicio a través de Internet, lo que implica la transferencia de actividades de tratamiento de datos a los sistemas del proveedor de servicios. Desde el punto de vista de la protección de datos personales, la consecuencia más destacable del uso de este tipo de nube es que el responsable del tratamiento está obligado a transferir una parte importante del control que ejerce sobre dichos datos y el proveedor de servicios desempeña un papel clave en lo que refiere a la protección eficaz de los datos personales almacenados en sus sistemas.

Por último, además de las nubes «públicas» y «privadas» encontramos **«nubes híbridas»**, donde el usuario es propietario de parte de la infraestructura y combina esta modalidad con servicios adquiridos en nubes públicas.

Como mencionamos anteriormente entendemos que las soluciones tecnológicas no son neutras y, si analizamos la estructura de cada modelo, encontramos una tensión importante entre los **enfoques orientados a optimizar costes (perdiendo el control sobre la infraestructura y los datos) y el enfoque orientado a garantizar los derechos de los usuarios**. Lamentablemente, para muchas instituciones no es viable o sostenible a largo plazo el uso de una nube privada, principalmente por razón de costes. En cuanto a la conveniencia de la adopción de un modelo u otro, aquí no encontramos una respuesta única, aunque consideramos que al Estado, a través de las Unidades

Nacionales de Protección de Datos, le corresponde apoyar a las Instituciones Educativas al momento de tomar este tipo de decisiones y proporcionar elementos para evaluar opciones.

Para lograr una primera aproximación al tema de la contratación y subcontratación de servicios cloud por parte de IEs, y dado que en Uruguay no contamos con relevamientos sobre el tema, podemos tomar los datos de la "*Primera inspección sectorial de oficio sobre servicios del cloud computing en el ámbito educativo*" publicada por la Agencia Española de Protección de Datos en el año 2015. De los resultados de dicha inspección se deriva que, en el ámbito educativo español, la oferta de servicios cloud es compleja, existiendo múltiples actores cumpliendo diferentes roles. Del mismo relevamiento surge evidencia de que para el caso español:

- La mayoría de las empresas especializadas en aplicaciones educativas utilizan los servicios de infraestructura de nube de entidades prestadoras de estos servicios, no habiendo desarrollado infraestructuras propias.
- Cada vez más empresas multinacionales, no especializadas en educación, ofrecen además plataformas de aprendizaje utilizando su propia infraestructura de nube.

Al finalizar nuestra investigación esperamos aportar mayor información sobre el uso de plataformas educativas en la nube en el contexto nacional.
A continuación, relevaremos el marco legal aplicable a este tipo de soluciones en materia de protección de datos personales.

## 3 - Las Instituciones Educativas como responsables del tratamiento de datos

En la Ley 18.331 de Protección de Datos Personales[3] (LPDP) encontramos dos conceptos centrales para el análisis de la responsabilidad de las partes implicadas en la computación en la nube, estos

3Nuestra LPDP considera como dato personal a cualquier tipo de información referida a una persona que la pueda identificar directamente o indirectamente, (como nuestro nombre, dirección, teléfono, cédula de identidad, RUT, huella digital, etc.) y regula de forma particular aquellos datos considerados sensibles (artículo 18)

son los de “responsable de tratamiento” y “encargado del tratamiento”:

**Responsable de la base de datos o del tratamiento:** persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento. (artículo 4 Lit. K LPDP)
**Encargado del tratamiento**: persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento (artículo 4 Lit. H LPDP).

Las IEs, como responsables del tratamiento de los datos de estudiantes y docentes, deben cerciorarse de que sus datos personales sean tratados conforme a derecho (principio de responsabilidad artículo 12 LPDP). Esto implica que tienen la responsabilidad de garantizar que su proveedor de servicio en la nube cumple con la LPDP. Será fundamental entonces que presten especial atención a las características de los contratos y a las cláusulas relativas al procesamiento de datos.

Entre las responsabilidades de las IEs encontramos las siguientes:

- Recabar el consentimiento previo e informado de docentes y estudiantes especificando de forma clara para qué serán utilizados sus datos (principio de finalidad) y quién podrá acceder a ellos.
- Recabar el consentimiento parental cuando se trate de servicios de nube que implique el tratamiento de datos personales de menores de edad.
- Supervisar el tratamiento de datos garantizando que sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines.
- Garantizar la confidencialidad de los datos, debiendo seleccionar un proveedor de servicio en la nube que reúna garantías y medidas de seguridad suficientes.
- Garantizar la Integridad de los datos.

- Brindar a los usuarios una vía ágil para ejercer los derechos de acceso, rectificación, supresión e impugnación de sus datos personales.
- Registrar las bases de datos personales en el registro de bases de la URCDP (Unidad reguladora y de Control de Datos Personales de AGESIC).
- Proporcionar una política de privacidad con términos claros y comprensibles.
- Evitar el uso no autorizado de datos, por ejemplo, el uso con fines publicitarios.
- Comprobar que sus proveedores cumplen con las normas de transferencias de datos fuera de fronteras.
- Garantizar la disponibilidad del servicio (acceso oportuno y confiable a los datos personales) comprobando que se han tomado medidas razonables para hacer frente a los riesgos de interrupciones.

## 4 - Los proveedores encargados del tratamiento

Los proveedores de servicios de nube (empresas nacionales o extranjeras) contratados por IEs nacionales deberán cumplir con las obligaciones previstas por la normativa nacional y cualquier cláusula contractual que disponga lo contrario será nula (artículo 3 del Decreto N° 414/009).

Los encargados del tratamiento también son responsables de:

- garantizar la confidencialidad (artículo 11 LPDP)
- la adopción de las normas de seguridad, de conformidad con las disposiciones de la LPDP (artículo 10) y el decreto 414/009 (artículos 7 y 8)[4].
- apoyar y asistir al responsable del tratamiento a respetar los derechos ejercidos por los interesados (LPDP artículo 10).
- garantizar que los datos se utilizan únicamente para el fin que figure en el contrato de servicio (LPDP artículo 30)
- supresión de los datos una vez finalice el contrato (LPDP artículo 30).

4Vale la pena destacar que ni la LPDP, ni su Decreto reglamentario establecen cuáles serán las normas de seguridad mínimas.

Si bien Uruguay no ha incorporado el *derecho a la portabilidad de datos* en su marco legal, es recomendable que el responsable del tratamiento incluya cláusulas de portabilidad e interoperabilidad al contratar proveedores. La portabilidad implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable. Cuando ello sea técnicamente posible, el responsable deberá transferir los datos directamente al nuevo responsable designado por el interesado.

## 5 - Las grandes corporaciones de la información y los servicios educativos en la nube

Para comprender la real dimensión de la problemática relacionada con la privacidad y los servicios educativos en la nube, no basta con comprender los aspectos técnicos y jurídicos, debemos incorporar otros datos de la realidad como las tendencias en el mercado de las tecnologías educativas y sus implicancias.

El campo de las tecnologías educativas parece estar reclamando en la actualidad la denominación de “industria” por derecho propio. Se habla de un mercado potencialmente gigantesco que no es tan sólo un subsector dentro de la industria del software. Según el informe de EdTechXGlobal, conferencia global de negocios en tecnología educativa, aunque se calcula que solamente el 2% de la educación está digitalizada, el mercado actual estaría creciendo a una tasa de 17% anual y alcanzaría el valor de 252 mil millones de dólares en 2020[5]. Cifras millonarias similares a estas se repiten en los medios especializados de este sector, con considerables variaciones en su magnitud, pero siempre desde una narrativa que hace énfasis en el potencial de este codiciado mercado educativo. Fundaciones y fondos de capital de riesgo están invirtiendo grandes sumas en las “startups educativas”.[6] Anualmente se realizan sendas listas de las tecnologías más “innovadoras” y

5Fuente: http://www.marketwatch.com/story/global-report-predicts-edtech-spend-to-reach-252bn-by-2020-2016-05-25-4203228
6Según el informe 2015 de CB Insights sobre financiamiento de empresas de tecnología educativa, las inversiones entre

“disrruptivas” en educación y se realizan todo tipo de proyecciones, con un enfoque más financiero que educativo[7], acerca del progreso de este sector. Aunque esta industria está muy desarrollada en EEUU y Europa, las inversiones son atraídas cada vez más por las llamadas economías emergentes, especialmente en Asia, donde se considera que habrá un mayor crecimiento de la demanda en tecnologías educativas.[8]

Dentro de esta industria destacan algunas compañías nacidas como startups educativas, como Udacity, Coursera, Edmodo y otras, valoradas en millones de dólares. El sector también comprende tecnologías y proyectos libres con modelos de negocio abiertos, como Moodle, de amplio uso para la gestión de aulas virtuales. Sin embargo, también están desarrollando sus negocios en esta área grandes corporaciones: Google, Apple, Amazon, Microsoft y Facebook, que desarrollan productos con sus marcas o adquieren y financian startups.

Una y otra vez, en informes y análisis de consultoras, se repite que estas corporaciones aprovecharán “sus potentes plataformas”, “su ecosistema”, “su enorme base de usuarios” para imponerse en el ámbito educativo. No siempre se comenta que también se basan en una importante capacidad de lobby para ganarse grandes clientes institucionales, tanto de la educación pública como privada. Además, en muchas ocasiones las ofertas de productos de tecnologías educativas por parte de las corporaciones viene acompañado de una narrativa filantrópica[9]. Los vínculos entre ellas

---

2010 y 2014 tuvieron un crecimiento de 503%.

7Es muy interesante la crítica a la mitología de la disrrupción en educación realizada por Audrey Watters: http://hackeducation.com/2013/05/24/disruptive-innovation

8Sobre el “boom” de la inversión en tecnologías educativas en China: https://www.cbinsights.com/blog/chinas-booming-ed-tech-industry/

9Como antecedentes podemos nombrar la estrategia de la Compañía Google que provee la suite Google Apps for Education de forma gratuita al sistema educativo público de varios países en desarrollo. En el 2012 firma un acuerdo con el Dpto de Educación de Filipinas http://googleforwork.blogspot.com.uy/2012/09/islands-in-cloud-philippines-department.html?m=1
En el 2013 el gobierno con el gobierno de Malasia (10 millones de cuentas en total: https://venturebeat.com/2013/04/10/google-10-million-malaysian-students-teachers-and-parents-will-now-use-google-apps-for-education/
Finalmente, en el año 2015, firma convenio con el Plan Ceibal para ofrecer esta suite a los estudiantes de primaria y secundaria de Educación Pública de Uruguay: https://www.presidencia.gub.uy/comunicacion/comunicacionnoticias/ceibal-suma-herramientas-google-potenciar-trabajo-docentes-estudiantes

y los gobiernos se inician muchas veces como acciones de cooperación para mejorar la educación y brindar acceso universal a herramientas e incluso conectividad a poblaciones con carencias.

Particularmente los programas gubernamentales de tecnología en la educación son un *target* preferido en este negocio, que implica contratos para proveer dispositivos, aplicaciones y contenidos a todo el sistema público. Pero su principal negocio no pasa necesariamente por las compras y contratos institucionales o estatales, sino por la articulación del negocio de tecnología educativa con sus objetivos de negocios centrales: la explotación del *big data* (Google, Facebook), la imposición de marca de un determinado sistema operativo (Microsfot con Windows, Google con Android, Apple con iOS) o de un ecosistema cerrado en torno a sus dispositivos (iPad de Apple, Chromebook de Google, Kindle de Amazon).[10]

La preocupación por la privacidad y la protección de datos en educación ha surgido como debate público a partir de la irrupción de estas grandes corporaciones en educación. Del mismo modo en que han crecido los cuestionamientos sobre el tratamiento de los datos personales en los servicios online en general, la aceptación de términos y condiciones difíciles de entender y el escaso control de los usuarios sobre sus datos, han suscitado críticas y temores, especialmente justificados cuando se trata de servicios educativos.

Estas preocupaciones, expresadas por distinto tipo de actores, se ven reflejadas en informes gubernamentales, como el realizado por la Agencia Española de Protección de Datos Personales[11], o en análisis críticos desarrollados por organizaciones no gubernamentales, como las preguntas

10Incluso la cobertura mediática más complaciente respecto al *edtech bussiness*, lanza este tipo de hipótesis: “Si Facebook creó un nuevo universo virtual de relaciones sociales, si Apple creó un ecosistema de hardware cerrado sobre sí mismo en base a incontables aplicaciones, si Google atrapó a casi toda la humanidad en su sistema de búsquedas, ¿no tendrán entre sus planes hacer algo similar dentro del mundo educativo? ¿Será un motor de búsqueda, un mercado de clases, una red social o un ecosistema de aplicaciones lo que controle el aprendizaje? ¿Competirán entre sí o se repartirán partes del proceso de aprendizaje como hoy sucede con la mayoría de sus negocios?” Fuente: http://futuroeducativo.com/ya-estan-aqui-como-entraron-en-la-educacion-google-apple-amazon-facebook-y-microsoft/

11Ver: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_07_22-ides-idphp.php

frecuentes acerca de servicios educativos en la nube y dispositivos en las escuelas de la EFF[12], o las campañas activistas de la Parent Coalition for Student Privacy en Estados Unidos[13]. En Uruguay este debate surgió por primera vez en la opinión pública a raíz de un acuerdo entre el Plan Ceibal y Google por el cual el primero accedía gratuitamente a los servicios de Google Apps For Education.

Estos debates ponen de relieve que, aunque los servicios educativos en la nube tienen grandes ventajas, también son notables sus riesgos desde la perspectiva de la protección de datos, exponiendo a los estudiantes a niveles de vigilancia difíciles de percibir y controlar. Analizaremos algunos de estos riesgos a continuación.

## 6 - Principales riesgos relacionados con la contratación de servicios en la nube

Las tecnologías educativas que se utilizan en las escuelas y universidades comprenden un amplio espectro de herramientas: desde dispositivos hasta aplicaciones, pasando por servicios de nube o "cloud". Estos servicios cloud pueden consistir en campus y aulas virtuales, de carácter específicamente educativo, así como en servicios de redes sociales, webmail y almacenamiento en la nube. Las grandes corporaciones de internet, como vimos antes, están fuertemente implicadas en este mercado, a través de servicios cloud como Google Apps For Education, o Microsoft in Education.

Como vimos antes, hay diversos modelos de implementación de estos servicios, que pueden ser provistos por la IE o subcontratados. Si bien en ambos casos, los servicios tienen que respetar la legislación vigente en materia de protección de datos, la subcontratación a terceros implica riesgos que hay que tener en cuenta especialmente. El Grupo de Trabajo sobre Protección de Datos del Artículo 29 de la Directiva 95/46/CE (Grupo del artículo 29[14]), detecta **dos riesgos principales[15]**,

12Ver: https://www.eff.org/issues/student-privacy/faq
13Ver: http://www.studentprivacymatters.org/
14Grupo que reúne a todos las Autoridades de Protección de Datos de los países de la UE.
15Dictamen 05/2012 sobre la computación en nube (Grupo del Artículo 29 - UE) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf

que habrá que evaluar de acuerdo al volumen de datos personales que se maneje, los usuarios alcanzados y el tipo de institución contratante de servicios de nube, estos son:

1. **Pérdida de control.** Esta puede expresarse de la siguiente manera: a) Falta de disponibilidad (dependencia respecto del proveedor), b) Falta de integridad (causada por la puesta en común de los recursos en la nube una nube pública), c) Falta de confidencialidad, d) Falta de posibilidad de intervención debido a la complejidad y la dinámica de la cadena de subcontratación, e) Falta de posibilidad de intervención, f) Falta de poder de negociación de las cláusulas contractuales (ya que las ofertas normalizadas son una característica de los servicios de computación en nube)

2. **Falta de información sobre el tratamiento (transparencia).** La ley obliga a que los interesados cuyos datos personales sean objeto de tratamiento en la nube sean informados acerca de la identidad del responsable del tratamiento y de los fines del tratamiento. La principal consecuencia de la falta de transparencia es que, la IE que contrata el servicio en la nube, muchas veces no es consciente de las amenazas y riesgos potenciales y, por tanto, no podrá adoptar las medidas de protección apropiadas. Los datos personales de los usuarios se encuentran en riesgo si la IE, por ejemplo, no sabe:
    - **a.** la composición de la cadena de los múltiples encargados del tratamiento y los subcontratistas,
    - **b.** si se transmiten datos personales a terceros países que pueden no proporcionar un nivel adecuado de protección de datos,
    - **c.** si las transferencias no cuentan con las medidas de protección adecuada.

Pero las IEs (y las Unidades de Protección de Datos de cada país) encaran un problema mayor que el del control de proveedores de servicios educativos basados en la nube, este problema es la **falta de adecuación de los actuales sistemas de protección de datos personales al tratamiento masivo de datos en el ámbito educativo o al “big data en educación”**.

Har Carmel (2016) resume los principales problemas que enfrentan los sistemas de protección de datos personales como el de Uruguay (basados en el modelo europeo). Primero, **el sistema no protege los datos de estudiantes de la re-identificación**, o sea, si definimos datos personales como "*datos que identifican o hacen identificable a una persona*", basta con anonimizar esos datos para que la ley deje de ser aplicable. El tema es que resulta bastante cuestionable concebir la anonimización cuando hablamos de "big data" debido a que las técnicas de agregación, derivación contextual y correlación cruzada de grandes volúmenes de información hacen que el riesgo de re-identificación del estudiante sea muy grande. Segundo, el principio rector de estos sistemas de protección de datos, es el principio del previo consentimiento informado. Aunque excluyamos la posibilidad de ambigüedad en la información proporcionada a los padres por parte de empresas proveedoras de servicios, **difícilmente podremos hablar de consentimiento informado** frente a la actual capacidad de usos secundarios basados en minería de datos (¡inclusive con fines de mejora en los procesos educativos!). **Será simplemente demasiado complicado para el padre promedio hacer elecciones conscientes frente al uso inesperado de los datos de los estudiantes**. Y por último, Har Carmel también plantea la **imposibilidad de los padres de negarse (opt-out) a brindar su consentimiento**, debido a las consecuencias que deberá afrontar si decide no acompañar la decisión de la IE en cuanto a la selección de proveedores y a la política de privacidad de estos proveedores, ya que no todos los padres tienen la posibilidad de cambiar de IE a sus hijos.

Podemos concluir que, estamos frente a un cambio de paradigma y que, sin lugar a dudas, nos enfrentamos a la necesidad de superar el enfoque de auto-gestión [16] por parte del usuario en la protección de sus datos personales y privacidad. Solove (2013) y Har Camel (2016) plantean la re evaluación del equilibrio de intereses entre sujetos de datos y usuarios de datos mediante un enfoque que considera la privacidad y la protección de datos personales como un nuevo interés

16Este enfoque de auto-gestión se encuentra muy arraigado en las Unidades de Protección de Datos Personales de todo el mundo. Prueba de ello es el último párrafo del Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas): *"A los niños se les hará conscientes de que son ellos mismos los primeros protectores de sus datos personales. Con arreglo a este criterio, la participación gradual de los niños en la protección de sus datos personales (desde la consulta a la decisión) se hará efectiva. En este ámbito, la efectividad de las condiciones creadas para el ejercicio pleno de los derechos puede demostrarse."*

colectivo que requeriría una nueva combinación de regulación pública y gestión privada para aumentar el nivel real de protección de la privacidad de los estudiantes.

## 7 - Recomendaciones para la Contratación de servicios de nube para Educación

En Uruguay aún no contamos con estudios, evaluaciones de impacto o inspecciones sectoriales oficiales publicadas por la URCDP - Agesic, describiendo la situación de la protección de datos personales en el sector educativo y advirtiendo los riesgos y cuidados que las IEs deberían tomar en cuenta al momento de contratar servicios cloud.

En Europa, las Autoridades de Protección de Datos de cada país de Europa han realizado inspecciones sectoriales y han elaborado guías para efectivizar el cumplimiento de la Directiva Europea de Protección de Datos, recogiendo y ampliando las recomendaciones del *Dictamen 05/2012 sobre la computación en nube* del Grupo del Artículo 29 - UE. En lo referente al ámbito estrictamente educativo encontramos que, en octubre de 2014 la ICO, Autoridad de Protección de Datos de Reino Unido publica su *"Cloud (educational apps) software services and the Data Protection Act"* y que en el mes de julio del 2015 España ha publicado los resultados de la *"Primera inspección sectorial en Europa sobre servicios del cloud computing en el ámbito educativo"*, estos documentos constituyen los insumos fundamentales de las recomendaciones que resumimos a continuación:

**Necesidad de evaluar Impacto en Privacidad**. Antes de contratar debería ser preceptivo que las IEs efectúen una evaluación de conveniencia e impacto. La ICO, Autoridad de Datos del Reino Unido, recomienda a los centros educativos la evaluación de las plataformas y servicios de nube mediante una herramienta denominada *PIA: Privacy impact assessment* a los efectos de identificar y minimizar los riesgos relacionados con cuestiones de privacidad en nuevos proyectos y políticas que involucren la contratación de servicios o plataformas en la nube.

**Contratos con garantías.** Los centros educativos deberán formalizar la contratación de servicios de nube de forma que puedan acreditar su celebración y la incorporación de las garantías adecuadas para la protección de datos personales, incluidas las exigibles en caso de subcontratación. Asimismo, el prestador de servicios de nube debe garantizar la portabilidad de la información y la no conservación de los datos al término del contrato (borrado seguro).

**Ubicación de los datos y sub procesadores.** Es necesario que los centros educativos conozcan las entidades que intervienen en la prestación de servicios de nube, su ubicación y las garantías adoptadas en caso de que vayan a realizarse transferencias internacionales de datos.

**Posibilidad de auditoría.** Es preciso que en el contrato se establezca el método o, al menos, la posibilidad de que el centro educativo realice auditorías. El responsable del tratamiento debe mantener el control sobre los datos.

**Responsabilidades en materia de seguridad.** Es preciso especificar claramente las responsabilidades de todos los intervinientes (IEs, servicios de alojamiento y plataformas educativas) en la implantación de las medidas de seguridad. En particular, hay que asegurar la adecuada asignación de permisos de acceso a los datos personales y concienciar a los usuarios sobre los peligros de utilizar contraseñas que no sean suficientemente robustas.

## 8 - Conclusiones

A medida que vamos avanzando con nuestra investigación ("Privacidad y protección de datos en la educación pública uruguaya"), hemos constatado que en Uruguay queda aún mucho camino por recorrer en materia de protección de datos personales y privacidad de plataformas educativas. Consideramos que la información sobre riesgos y las recomendaciones presentadas en este artículo podrán ser de utilidad para que las IEs (tanto públicas como privadas) tomen decisiones informadas al momento de contratar servicios educativos en la nube.

Entendemos que la opción de tecnología cloud que implica menor riesgo desde la perspectiva de la privacidad y protección de datos personales será la generación de infraestructura propia de nube privada dedicada a la institución, siempre que ésta sea acompañada de una buena gestión de privacidad que incluya una política de privacidad expresa, no ambigua y limitada estrictamente a los fines de la IE, acompañada de medidas de seguridad suficientes y el registro de las bases de datos para su control por la URCDP.

De cualquier forma, debido a que no todas las instituciones educativas uruguayas optan por gestionar su propia infraestructura y al avance de la oferta de servicios cloud para educación, consideramos que sería de utilidad:

- Que las instituciones educativas utilicen el mecanismo de consulta que ofrece la Unidad Reguladora y de Control de Datos Personales (URCDP) de AGESIC, solicitando asesoramiento previo a la contratación de servicios en la nube.
- Contar con guías oficiales de evaluación de impacto de las plataformas y servicios de nube destinadas a los tomadores de decisiones de las IEs de Uruguay.
- Contar con inspecciones o relevamientos oficiales nacionales (por parte de la URCDP) para servicios de nube en el sector educativo en Uruguay.

Finalmente, entendemos que persiste el problema de la falta de adecuación de nuestro sistema de protección de datos personales al tratamiento masivo de datos en el ámbito educativo o al “big data en educación”, ya que nuestro sistema se basa en el principio del “consentimiento previo informado” o la “autogestión de la privacidad”, ficción jurídica que, como hemos visto, se encuentra cada vez más alejada de la realidad. La búsqueda de una solución a este problema implicaría una revisión del marco jurídico nacional aplicable.

## Bibliografía

AEDP - España, “*Guía de servicios para contratación de servicios de cloud computing”, disponible en*: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

AEDP - España, “*Primera inspección sectorial en Europa sobre servicios del cloud computing en el ámbito educativo*”, julio de 2015, disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Inspeccion_cloud_educacion.pdf

Grupo del Artículo 29 - UE, “*Dictamen 05/2012 sobre la computación en nube”, disponible en* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf

Har Carmel, Y. (2016). Regulating “big data education” in Europe: lessons learned from the US. Internet Policy Review, 5(1). DOI: 10.14763/2016.1.402

ICO - UK, “*Cloud (educational apps) software services and the Data Protection Act*”, disponible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/608686/Cloud-services-software-dept-advice_26.pdf

Mell, Peter and Grance, Timothy “The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology.” Computer Security Division, U.S. Department of Commerce, setiembre de 2011. Disponible en: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Solove, D. J. (1880). Introduction: Privacy Self-Management and the Consent Dilemma. 126 Harv. L. Rev.

Vance, Amelia, “National Association of State Boards of Education - Trends in Student Data

Privacy Bills in 2016", Policy Updates, Vol. 23, Nº 13, Mayo 2016. Disponible en: http://www.nasbe.org/wp-content/uploads/Vance_2016-State-Final.pdf